AMC Supplement 1 to AR 380-53

Security:

Information Systems Security Monitoring

U.S. Army Materiel Command
9301 Chapek Road
Fort Belvoir, VA 22060-5527
2 August 2005

UNCLASSIFIED

SUMMARY of CHANGE

AMC Supplement 1 to AR 380-53, AMC Information Systems Security Monitoring

This revision –

- This supplement is updated for administrative purposes only.

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
9301 CHAPEK ROAD, FORT BELVOIR, VA 22060-5527

AMC Supplement 1 to AR 380-53 — 2 August 2005

Security

INFORMATION SYSTEMS SECURITY MONITORING

This supplement applies to Headquarters, Army Materiel Command (AMC), AMC Major Subordinate Commands (MSC), and Separate Reporting Activities (SRA). It prescribes policies and procedures for establishing and managing an AMC Information Systems Security (ISS) Monitoring program.

This supplement may NOT be further supplemented without prior written approval from the Deputy Chief of Staff, G-2, Headquarters, U.S. Army Materiel Command. One copy of all approved supplements will be provided to the DCS, G-2, ATTN: AMXMI-SCM.

AR 380-53, dated 29 April 1998 is supplemented as follows:

Page 2. Paragraph 1-4i, Commanders of MACOMs. Add the following as paragraphs 1-4i(5) and (6).

(5) Within the Army Materiel Command, the Commanding General's single designee for Information Systems Security Monitoring is the DCS, G-2. The DCS, G-2 will:

(a) Prepare, publish and maintain AMC ISS monitoring policy.

(b) Review and forward to Headquarters, Department of the Army, all requests for ISS monitoring, including any network penetration, testing and verification conducted as part of a Computer Defense Assistance Program (CDAP), within the National Capitol Region (NCR) (see also para 2-10b, basic regulation).

(c) Review and approve techniques and procedures for conducting ISS monitoring in AMC.

(d) Certify personnel who are to supervise or conduct ISS monitoring (see para 3-3d & e, basic regulation).

(e) Ensure notification procedures for ISS monitoring, as provided in para 2-5, basic regulation, are implemented and adhered to.

(f) Ensure personnel authorized to conduct ISS monitoring comply with the provisions of AR 380-53 and this supplement.

---

*This supplement supersedes AMC Suppl 1 to AR 380-53, 20 March 2003

(g) Ensure products of ISS monitoring are used for their intended purposes only.

(h) Coordinate all MSC and SRA related ISS monitoring issues within the Headquarters, and, as required, with HQDA.

(i) Provide security oversight for ISS monitoring throughout the Command. This will be done through security assistance visits and Security Support Division (SSD) inspections.

(j) Perform biennial certification of notification procedure actions under chapter 2, basic regulation.

Page 2, Paragraph 1-4i(6): Add the following as paragraph 1-4i(6):

(6) The AMC CIO/G-6 (Chief Information Officer) will coordinate all Computer Defense Assistance Program (CDAP) requests that include network penetration, testing and verification (Phases 5 and 6 in the CDAP Process are network exploitation and technical support) with the DCS, G-2 to ensure they meet the requirements of AR 380-53.

Page 2, Paragraph 1-4j, Commanders at all levels. Add the following as paragraph 1-4j(7):

(7) All AMC MSC Commanders and SRA directors will appoint a single designee to act as the focal point for all ISS monitoring within that command or activity. The name, grade, office symbol, mailing address, telephone number and e-mail address of each designee must be provided to HQ, AMC, ATTN: AMXMI-SCM. This information will be updated whenever a change occurs.

Page 2. Paragraph 2-2 Objectives. Add the following as paragraphs i through l:

i. To improve the ISS posture of AMC units and organizations by ensuring that only non-sensitive unclassified defense information is discussed or transmitted over or processed by non-secure information systems.

j. Determine the effectiveness of the security education and training programs. All personnel should realize information systems security monitoring is an ‘after the fact’ function. If items of a sensitive or classified nature are discussed or transmitted on a non-secure system, the information is lost, whether or not a friendly monitoring element noted it. The AMC goal is awareness, protection, and emphasis on using our information systems correctly to deny any unauthorized person, group, or nation information that may be used to harm us.

k. Provide an effective tool to enhance force protection.

l. Require all AMC personnel to employ secure information systems.

Page 3, paragraph 2-4, Certification of notification procedures. Add the following at the end of the first sentence in paragraph 2-4a:

MSC Commanders will ensure requests for certification arrive at the AMC DCS, G-2 no later than 1 July of each odd-numbered year.

Page 4. Paragraph 2-6, Conduct of Information Systems Security Monitoring. Add the following as paragraphs e & f:

e. ISS monitoring will NOT be conducted on any telecommunications containing privileged doctor-patient, lawyer-client, chaplain-petitioner, or Inspector General communications.

f. The AMC DCS, G-2 will be notified of all ISS monitoring conducted within the command a minimum of 30 days PRIOR to commencement of the monitoring.

Page 5, Paragraph 2-10, Prohibitions on Information Systems Security Monitoring. Add the following at the end of paragraph 2-10b:

All requests for ISS monitoring within the NCR will arrive at the AMC DCS, G-2 a minimum of 60 days prior to the date monitoring is desired.

Page 5, Paragraph 2-10d. Add the following at the end of paragraph 2-10d:

All requests for ISS monitoring of official government telecommunications systems outside DOD will arrive at the AMC DCS, G-2 a minimum of 60 days prior to the date monitoring is desired.

Page 5, paragraph 2-10e(1). Add the following at the end of paragraph 2-10e(1):

All requests for ISS monitoring of U.S. Government contractors at their own facilities will arrive at the AMC DCS, G-2 a minimum of 60 days prior to the date monitoring is desired.

Page 5, paragraph 2-10e(2). Add the following at the end of paragraph 2-10e(2):

For all AMC organizations and activities, this request will be reviewed by supporting Command Counsel, Chief Counsel, or Staff Judge Advocate Office.

Page 5, paragraph 2-10g. Add the following at the end of paragraph 2-10g:

Any requests by AMC activities to monitor the telecommunications of other MACOMs or DOD components will be forwarded to the AMC DCS, G-2 a minimum of 60 days prior to the date monitoring is desired.

Page 5, paragraph 2-10i. Add the following at the end of paragraph 2-10i:

…as well as Inspector General communications.

Page 6, paragraph 2-10l. Add the following at the end of paragraph 2-10l:

Requests for exception, fully justified, will arrive at AMC DCS, G-2 a minimum of 60 days prior to the date monitoring is desired.

Page 6, paragraphs 3-3, Training and standards for Information Systems Security Monitoring. The following will be added at the end of paragraph 3-3d(1):

A copy of this certification will also be maintained on file in the MSC Command security office.

Page 6, paragraph 3-3e(3). Add the following to paragraph 3-3e(3):

Requests to use untrained personnel will arrive at the AMC DCS, G-2 a minimum of 30 days before the desired date monitoring operations are to commence.

Page 6, paragraph 3-3j. Add the following between "be" and "granted": ...requested through command channels and...

Page 7, paragraph 3-5, Information Systems Security Monitoring working materials. Add paragraphs (1) & (2) at the end of paragraph 3-5f:

(1) AMC monitoring activities wishing to maintain ISS working materials longer than 30 days must provide a fully justified request in writing to the AMC DCS, G-2 no less than five working days before the end of the original 30-day period.

(2) All requests to maintain ISS working materials beyond the additional 30 days referred to above will arrive at AMC DCS, G-2 a minimum of 15 working days prior to the end of the AMC approved 30-day extension.

Page 8, paragraph 4-2a. Add the following after the words "Command channels" in the second sentence: (with an information copy to HQ, AMC ATTN: AMXMI).

The proponent for this supplement is the Deputy Chief of Staff, G-2, U.S. Army Materiel Command. Users are invited to send comments and suggestions for improvement in DA Form 2028 format to the Commander, USAMC, ATTN: AMXMI -SCD, 9301 Chapek Road, Fort Belvoir, VA 22060-5527.

//Signed//
RICHARD A. HACK
Lieutenant General, USA
Deputy Commanding General

DISTRIBUTION:
B
H